RFC 7021 : Assessing the Impact of Carrier-Grade NAT on Network Applications

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 20 septembre 2013

Date de publication du RFC : Septembre 2013

https://www.bortzmeyer.org/7021.html

Sous le nom générique (et souvent erroné) de NAT se trouve tout un zoo <https://www.bortzmeyer.org/nats.html> de techniques variées et n'ayant en commun que leur complexité et leur fragilité. Ce nouveau RFC documente les problèmes liés à une technique particulière, nommée « double NAT » ou « NAT 444 » ou encore « CGN ». Lorsqu'un malheureux paquet IP subit **deux** traductions, qu'est-ce qui va casser ?

L'idée du CGN (un terme marketing, qu'il vaudrait mieux remplacer par NAT 444 pour « deux NAT sur le trajet d'un paquet IPv4 ») est de faire beaucoup d'efforts et de dépenser beaucoup d'argent pour ne **pas** migrer vers IPv6. Au lieu de déployer IPv6, ce qui simplifierait beaucoup les choses, notamment pour les applications, on déploie de gros routeurs NAT chez le FAI (loin des utilisateurs, d'où le nom de CGN - "*Carrier-Grade NAT*" - par opposition au NAT CPE des "*boxes*" actuelles). En toute rigueur, on peut avoir du CGN sans avoir du double NAT (c'est par exemple courant dans les offres 3G). Mais ce RFC se focalise sur le cas typique de l'accès Internet à la maison ou au bureau où les paquets IPv4 subiront une double traduction, par une "*box*" chez le client puis par le routeur CGN chez le FAI. On aura donc deux NAT à la suite.

Ce RFC n'est pas une analyse théorique. Au contraire, il décrit le résultat de tests effectifs menés par un labo des FAI et deux FAI importants (CableLabs, Time Warner Cable et Rogers), qui ont testé en vrai le NAT 444 et les problèmes qu'il pose. La première campagne de tests a été faite en 2010 et avait montré que des applications comme le "*streaming*" vidéo, les jeux en ligne et le partage de fichiers en pair-à-pair avaient des ennuis. Une seconde série de tests a été faite en 2011 par CableLabs seul, en essayant du matériel de plusieurs vendeurs (A10, Juniper, Alcatel-Lucent) pour faire le CGN. D'une manière générale, les tests n'ont été faits qu'avec les applications qui avaient des chances (ou plutôt des malchances) d'avoir des problèmes : un simple accès en lecture seule à une page Web ordinaire ne présente pas de risques et n'a donc pas été testé. La liste des applications testées est longue ;

— Distribution de vidéo depuis Netflix, YouTube et d'autres,

— Applications pair-à-pair comme le partage de fichiers avec BitTorrent en se servant du logiciel [Caractère Unicode non montré [1]]Torrent,
— Jeux en ligne avec Xbox,
— Transferts de fichier en FTP,
— Téléphonie avec SIP (avec des logiciels comme X-Lite ou PJSIP <http://www.pjsip.org/>) ou avec le système fermé Skype,
— Réseaux sociaux comme Facebook,
— Conférence à distance par exemple avec WebEx,
— Et plusieurs autres.

Ce RFC est essentiellement consacré à rendre compte des résultats de cette seconde campagne de tests.

La section 2 du RFC commence par décrire les architectures utilisés pour les tests. Par exemple, le premier cas (section 2.1.1) est le cas le plus simple : une seule machine terminale (« client »), un seul réseau local, un seul FAI. Le deuxième cas correspond à une maison avec plus d'équipements puisqu'il y a deux machines terminales. Tous les cas avec deux machines chez l'utilisateur permettent de tester des applications pair-à-pair entre ces deux machines. Le troisième cas a deux réseaux locaux mais un seul FAI donc, avec le CGN, possibilité que les machines des deux réseaux se présentent à l'extérieur avec la même adresse publique (voir le cas des Xbox plus loin). Et le quatrième cas a deux machines terminales, chez des FAI différents (donc avec des routeurs CGN différents et des adresses IP différentes).

Divers petits routeurs ont été utilisés comme CPE pendant les tests (Netgear, Linksys, etc). Les machines terminales étaient des ordinateurs Windows ou Mac OS, des consoles Xbox, des tablettes iPad, des lecteurs Blu-Ray connectés, etc.

Résultats ? Les activités les plus traditionnelles comme envoyer et recevoir du courrier, ou comme lire le Web, n'ont pas été affectées par le CGN. Les technologies de transition vers IPv6 comme 6to4 (RFC 3056 [2]) avaient été testées lors des essais de 2010 et les résultats étaient très mauvais. Ces tests n'ont pas été refaits en 2011. Autrement, qu'est-ce qui n'a pas marché ?

Plusieurs applications pair-à-pair par exemple de jeu en ligne ou de téléphonie SIP ont échoué dès qu'un CGN était là. Dans le cas de la Xbox, deux utilisateurs situés chez le même FAI n'arrivent pas à se connecter entre eux s'il y a du NAT444. Cela a apparemment été réglé par Microsoft dans une mise à jour de décembre 2011. Dans le cas de PJSIP <http://www.pjsip.org/>, les appels passant par un fournisseur SIP marchaient mais pas ceux effectués en pair-à-pair.

[Caractère Unicode non montré]Torrent a fonctionné dans certains cas mais pas dans tous. Il utilise une variété de techniques pour passer à travers les NAT (y compris STUN).

Pourquoi ces échecs, lorsque ça marche avec du NAT « habituel » ? Il existe plusieurs raisons (analysées dans le RFC) mais, pour prendre l'exemple de la Xbox, c'est parce que le serveur des Xbox sait dire à deux consoles qui se connectent depuis la même adresse IPv4 publique : « vous êtes toutes les deux derrière un routeur NAT, communiquez directement sur vos adresses privées ». Cela fonctionne si les deux Xbox sont sur le même réseau local et peuvent en effet se parler sans intermédiaire. Mais s'il y a du CGN, et qu'elles sont sur des réseaux locaux différents, connectés par le même FAI, elles présentent au serveur de Microsoft la même adresse IPv4 publique mais elles ne peuvent pas se joindre avec leurs adresses privées.

1. Car trop difficile à faire afficher par LaTeX
2. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3056.txt

Les tests ont été qualitatifs (ça marche ou ça ne marche pas) mais aussi quantitatifs avec mesure de la latence <https://www.bortzmeyer.org/latence.html> ou de la gigue, pour lesquelles le CGN ne semble pas avoir d'impact négatif.

Soyons optimistes, il y a eu des améliorations entre les tests de 2010 et ceux de 2011, notamment grâce à l'utilisation plus fréquente de STUN ou de relais permettant de contourner les problèmes du NAT. Le RFC ne parle pas de l'aspect économique mais je note que, lorsqu'on évalue le coût des CGN, il faut voir que c'est aux auteurs d'application de payer pour les FAI, en augmentant la complexité de leurs applications pour contourner les obstacles.

Certains problèmes restent et semblent consubstantiels du CGN, comme la difficulté qu'il y a à fournir des informations aux autorités en cas d'enquête sur un comportement anormal : l'adresse IP publique qui est vue par les serveurs distants est partagée entre un grand nombre d'utilisateurs (RFC 6269).

Les résultats bruts des tests de 2010 figurent en section 5 et ceux des tests de 2011 en section 4, sous forme de tableau indiquant ce qui marche et ce qui ne marche pas.

Que recommander après ces résultats ? La section 6 traite de la gestion de ces problèmes liés au double NAT. Elle recommande notamment l'utilisation de PCP ("*Port Control Protocol*", RFC 6887), pour que les applications puissent ouvrir les ports nécessaires dans le routeur CGN.

Un exposé de CableLabs résumant leurs observations est disponible en « "*Carrier Grade NAT - Observations and Recommendations*" <http://rmv6tf.org/wp-content/uploads/2012/11/CGN_Observations_Recomendations-NAv6S_20121.pdf> ».